REMARKS

Reconsideration of this application is requested.

1. Examiner has objected to the specification for failure to include section headings. The specification has been amended to include appropriate headings. Removal of this objection is requested.

2. Examiner has rejected claims 1-8 under 35 USC 112 first paragraph, as failing to comply with the enablement requirement. More specifically, the Examiner states that

> "applicant's specification is non-enabling in regards to the security element comprising the decryption circuit...it is unclear how the decryption circuit can be used to "sign" (decrypt) the digital data, if the digital data has not been encrypted prior to the decryption process. The Examiner notes that decryption is defined as the process of restoring encrypted data. Therefore, in order to perform decryption of digital data, the data must be in encrypted form..."

As a preliminary matter, Applicant has cancelled claims 1-8 without prejudice, and has added new claims 9-16 consistent with U.S. format that more clearly define Applicant's invention.

Furthermore, Applicant has amended the specification and wishes to thank the Examiner for pointing out this obvious error in the present patent specification. Upon review of the application, it is clear that the terms "encrypt" and "decrypt" have been transposed inadvertantly at every location in the specification. Accordingly, the specification has been amended (via substitute specification) to correct this error. One of ordinary skill in the art, upon reading the application in its context, would

recognize this obvious error and it's correction. Further evidence of the anomaly and it's obvious correction is found in the specification on page 1, lines 29-33 wherein it is stated

> The present invention relates to a device for authenticating the taking of pictures made up of digital data comprising a picture taking apparatus and a security element carrying out the signing of at least part of the digital data...

One of ordinary skill in the art would clearly recognize that the "signing of...digital data" involves the operation of a digital signature, which utilizes both hashing (via circuit 5 in FIG. 1, or in chip card 9 of FIG. 2) and encryption (via chip card 2 or 9 of FIGs. 1 & 2 respectively) using public key K1. Further support for recognition of this clear error is found on the first full paragraph of page 3 of the specification, which recites "Each datum $D(m1)_{K1}$ constitutes the signature of the datum m1 and hence of the fraction F1(VN) from which the datum m1 emanated."

With regard to the verification aspect of the digital signing, the first paragraph of page 5 recites that "Figure 3 represents, according to the invention, a device for authenticating digital images emanating from a picture taking device such as that represented in Figure 1 or in Figure 2." The authentication thus consists of necessarily decrypting the digitally signed data using a private key K2, as further disclosed from Figure 3 and the accompanying text on pages 5-6 of the specification.

Applicant submits that, pursuant to MPEP section 2163.07, "[a]n amendment to correct an obvious error does not constitute new matter where one skilled in the art would not only recognize the existence of the error in the specification, but also the appropriate correction." Accordingly, one of ordinary skill in the art, upon reading of the original specification, would recognize that a digitally

signed datum would necessarily be "encrypted" (not decrypted) using a public key, while verification of the data would necessarily constitute a "decryption" (not encryption) of the signed data to verify the signature, and thus realize that use of the terms "encrypt" and "decrypt" were merely transposed, such transposing having been remedied in the specification as amended herein. Accordingly, no new matter has been added to the application. Reconsideration and removal of this 35 USC 112 first paragraph rejection is requested.

Applicant has newly added claims 9-16 in the present application. In summary, the present invention concerns the authentication of digital images emanating from a device such as a camera, which shoots an event and a control unit which processes the signal coming from the camera. More specifically, the user of the camera is authenticated.

Inside the camera, at least a part of the digital signal is hashed and signed. The hashing represents an irreversible operation (i.e. one cannot recover the original signal from the hashed signal). The signature is realized by ciphering (encrypting) the hashed signal with the help of a chip card containing a secret key K1. A multiplexer located in the camera provides a signal at the output of the camera composed alternately of a clear signal and the signed signal (see Figure 1).

In the unit control, a demultiplexing circuit restores, on one hand, the clear signal and, on the other hand, the hashed and encrypted signal. The hashed and encrypted signal is decrypted so as to obtain a hashed signal. The clear signal received by the control unit is hashed in the same way as accomplished in the camera. The two hashed signals are then compared. According to the result of the comparison, the signal is authenticated or not.

The authentication according to the claimed invention is such that it guarantees that the images have been shot by a definite camera and are corresponding to a specific signature (user chip card). New claims 9-16 recite features and limitations associated with the aforementioned description and find ample support throughout the specification. The prior art of record fails to disclose or suggest, either singularly or in combination, each of the features and limitations recited in new claims 9-16. Allowance of claims 9-16 is respectfully requested.

In view of the foregoing, Applicant respectfully submits that claims 9-16 are in condition for allowance. Favorable reconsideration is requested.

If a telephone conference would be of assistance in advancing prosecution of the above-identified application, Applicants' undersigned Attorney invites the Examiner to telephone him at **609-919-4428**.

Respectfully Submitted

Date: September 18, 2003

Edward J. Howard
Registration No. 42,670
DUANE MORRIS LLP

THOMSON LICENSING INC.
Patent Operations
CN 5312
Princeton, NJ 08543-0028